REMARKS

Applicant has amended the Title from: "CONNECTION BASED DENIAL OF SERVICE DETECTION" to: "CONNECTION BASED DETECTION OF SCANNING ATTACKS." The amended title more closely corresponds to the subject matter of the instant claims. No new matter has been added.

The examiner rejected Claims 1-36 under 35 U.S.C. 102(e), as being anticipated by Malan (2002/0032871).

Claim 1

Applicant's claim 1 is allowable over Malan, since Malan neither describes nor suggests "A method of detecting scanning attacks." In addition, Malan neither describes nor suggests the features of: "adding host-pair connection records …, at the end of a short update period, accessing the connection table to determine new host pairs, determining the number of new host pairs added … over the update period; and if a host has made more than a first threshold number "C1" host pairs, and the number of host pairs … is smaller than the threshold number by a first factor value "C2", then indicating to a console that the new host is a scanner.

The examiner stated:

> **As per claim 1, Malan et al. discloses detecting scanning attacks[i.e. Dos attacks, 0028, 0057], adding host-pair connection records to a connection table each time a host accesses another host[0084]; at the end of a short update period, accessing the connection table to determine new host pairs; determining the number of new host pairs added to the table over the update period; and if a host has made more than a first threshold number "CI" host pairs, and the number of host pairs in the profile is smaller than the threshold number by a first factor value "C2", then indicating to a console that the new host is a scanner[0031, 0037, 0067, 0084].**

The examiner relies on paragraphs [0028] and [0057] from Malan, which are reproduced below:

> **[0028] In accordance with principles of the present invention, a system and method is provided for detecting, tracking and blocking DoS attacks, which can occur between local computer systems and/or between remote computer systems, network links, and/or routing systems over a computer network.**

> **[0057] Referring to FIG. 3, a system 5 for detecting, tracking and blocking DoS attacks is incorporated in the computer network system 10 in accordance with one embodiment of the present invention. The system 5 can be located on a single server computer (not shown), which is in communication with components of the computer network system 10 or distributed over a plurality of server computers (not shown), which are also in communication with components of the computer network system 10.**

Neither in these passages nor elsewhere in Malan is there any disclosure of techniques to detect a scanning attack or to identify a scanner. Rather, Malan is directed to detection of DOS (denial of service) attacks. DOS and Scanning attacks are different types of attacks, as Applicant notes in the specification.[1]

In addition, the examiner relies on paragraph [0084] from Malan, reproduced below:

> **[0084] Referring again to FIG. 5, during this SYN-packet flood attack, the collector 20 collects flow statistics related to the SYN-packets and stores the flow statistics in the buffer 20a, which is located on the collector 20. The buffer 20a normalizes the incoming flow-statistics to form records. The records are places into a shared table. The storm detector module 20b analyzes the records in this shared table and detects anomalous traffic. In this example, the storm detector 20b detects the pattern of records as a SYN-packet flood attack, because the number of records exceeds a predetermined threshold defined on the storm detector 20b. The storm profiler 20d also analyzes the records and based on this analysis, the storm profiler 20d adaptively adjusts the predetermined threshold defined on the storm detector 20b. After detecting the SYN-packet flood attack, the storm detector 20b sends an alert message along with a signature (e.g. a fingerprint of the alert) to the local controller 20f. The local controller 20f adds the signature of the alert to a table in memory, which represents the on-going local anomalies. When one of these local ongoing anomalies reaches a significant level of interest (e.g. a second predetermined threshold), such as a long duration or high severity, the local controller 20f notifies an anomaly-profiler module (not shown) to add a new anomaly to the set of current-anomalies that it measures. Thereafter, the anomaly-profiler module analyzes the normalized flow statistics in buffer 20a that are related to the anomaly and begins to collect long-term statistics about the anomaly. Furthermore, the anomaly-profiler places periodic snapshots of these long-term statistics into the storm profiler database 20e, which is located on the collector 20. At the same time, the local controller forwards the alert to the controller 24 as an alert message. The controller 24 can periodically request updated anomaly information, which in this example relates to a SYN-packet flood attack, from the local controller 20. The local controller 20 can respond by providing the controller 24 with the most recently collected long-term statistics related to the anomaly.**

Malan does not describe connection pairs. Rather, Malan discloses collection of data packet flow statistical information.[2] Nowhere does Malan describe that this information includes

[1] Specification page 7, lines 18-21; page 19, lines 2-7; page 22, lines 10-14 (as numbered in margin).

[2] Malan [0064] …. The data packet flow statisical information can include the number of packets which have been communicated between computer systems 16, the duration of communication between each of the computer

connection pair information nor does Malan disclose a connection table, or an equivalent structure. Accordingly, Malan neither describes nor suggests "adding host-pair connection records." Rather, Malan is directed to determining statistical information on packet flows. Accordingly, since Malan neither describes nor suggests "adding host-pair connection records", inherently Malan does not suggest, much less describe "... at the end of a short update period, accessing the connection table to determine new host pairs, determining the number of new host pairs added ... over the update period ... ." In addition, Malan neither describes nor suggests any approach for using this data from the connection table to determine if a host should be classified as a scanner. That is, claim 1, which also includes the features of "... if a host has made more than a first threshold number "C1" host pairs, and the number of host pairs ... is smaller than the threshold number by a first factor value "C2", then indicating to a console that the new host is a scanner.", is not suggested by any reading of Malan.[3]

Claim 2

Claim 2 recites that "..."C1" and "C2" are adjustable thresholds." While Malan discloses in [0084] that: "...the storm detector 20b detects the pattern of records as a SYN-packet flood attack, because the number of records exceeds a predetermined threshold defined on the storm detector 20b. The storm profiler 20d also analyzes the records and based on this analysis, the storm profiler 20d adaptively adjusts the predetermined threshold defined on the storm detector 20b." and "When one of these local ongoing anomalies reaches a significant level of interest (e.g. a second predetermined threshold), such as a long duration or high severity, the local controller 20f notifies an anomaly-profiler module (not shown) to add a new anomaly to the set of current-anomalies that it measures.", Malan does not disclose both the "predetermined

systems 16, the total number of packets communicated over each LAN (which is typically used for capacity planning) as well as other various data packet flow statistical information.

[3] Applicant's specification page 21, refers to these thresholds as C3 and C4, respectively. "The constants "C3" and "C4" are adjustable thresholds. This will catch most ping scans since typically a ping scan will scan many hosts in a short time."

threshold," which Malan teaches is adaptively adjusted by the storm detector, and "second predetermined threshold" as being "adjustable thresholds."[4]

Moreover, neither of the thresholds disclosed by Malan are "a first threshold number "C1" host pairs, and the number of host pairs is smaller than the threshold number by a first factor value "C2."

Claim 3

Claim 3 is distinct over Malan. The examiner argues that: "As per claim 3, Malan discloses wherein the connection table is a current time-slice connection table and host pair records are added to the current time slice connection table[0083-0084]." Applicant disagrees. Malan does not disclose to track connection pairs, and in particular host-pair records and does not disclose that the connection table is a current time-slice connection table.

Claim 4

Claim 4, the examiner contends that claim 4 is describes at [0029, 0032-0033, 0084]. Claim 4 calls for … aggregating records from the current time-slice table into a long update period table, checking for ping scans at the end of a long update period, and indicating hosts which produced more than "C3" new host pairs over the long update period.

At the outset, Malan does not address scanner attacks, per se and in particular the stealthy ping-type scanning attack.

The features of the current time-slice table, a long update period table, and checking for ping scans by indicating hosts which produced more than "C3" new host pairs over the long update period are not disclosed in Malan whether at [0029, 0032-0033, 0084] or elsewhere.

Claim 5

Claim 5 further limits claim 4. Claim 5 adds features of "… at the end of the long update period, accessing the long update connection table to determine new host pairs that the process had not determined before, determining the number of new host pairs added … over the long

[4] Id.

update period, and if … more than … "C4" host pairs, and the number of host pairs is smaller than …"C5", then indicating the new host as a scanner." Malan neither describes nor suggests these features not does Malan relate to scanners per se.

Claim 6

The examiner contends: "As per claim 6, Malan discloses maintaining Address Resolution Protocol (ARP) packet statistics in the connection table and for sparse subnets tracking the number of generated ARP requests that do not receive responses to detect scans on sparse sub-networks [0081-0082]."

Applicant contends that no such disclosure is found in Malan. [0081-0082] Malan is directed to discussion of the SYN-packet flood attack. Neither in these passages nor elsewhere is disclosed "maintaining Address Resolution Protocol (ARP) packet statistics … and for sparse subnets tracking the number of generated ARP requests that do not receive responses to detect scans on sparse sub-networks." Rather, the cited passages merely discuss aspects of the TCP connection protocol.

Claim 7

The examiner contends that: "As for claim 7, "Malan discloses wherein the scanning attack is a ping scanning attack [0081]." Claim 7 recites that "the scanning attack is a ping scanning attack." Malan neither describes nor suggests scanning attacks in general, and in particular a ping scanning attack. Rather, as mentioned above [0081] discloses a DOS (denial of service attack) which as pointed out above is different than a scanning attack.

Claim 8

Claim 8 is directed to a method of detecting port scanning attacks. As discussed above, Malan neither describes nor suggests detecting scanning attacks, in general, and in particular detecting port scanning attacks.

Claim 8 includes the features of "… retrieving … values of protocols and ports used in host pair connections … determining if the number of ports used in an historical profile is smaller by … than a current number of ports being scanned by a host, and if … greater … recording that the current number for the host is greater than a lower-bound threshold as an anomaly… ."

Malan neither describes nor suggests these features. While Malan discloses collection of statistical information, Malan does not disclose determining if the number of ports used in an historical profile is smaller by … than a current number of ports being scanned by a host.

The examiner contends that:

> **As per claim 8, Malan discloses detecting port scanning attacks, the method includes retrieving from a connection table logged values of protocols and ports used for host pair connections in the table [0042-0043, 0045]; determining if the number of ports used in the historical profile is considerably smaller by a factor "Cl" than a current number of ports being scanned by a host and the current number is greater than a lower-bound threshold "C2", to record the anomaly; and reporting a port scan to a console[0067-0068].**

As discussed above, Malan does not describe or suggest detecting port scans. Paragraphs [0042-0043, 0045] of Malan do not deal with retrieving logged values of protocol and ports used by host pair connections. Rather, those paragraphs are a discussion of collecting data statistics. While Malan also discusses processing data statistics to generate at least one record and "profiling the at least one record to generate a predetermined threshold.", as well as, "detecting if attributes related to the at least one record exceed the predetermined threshold representing the one or more data packet flow anomalies.", Malan again merely directed to DOS attacks and does not describe "logged values of protocol and ports used by host pair connections." None of the excerpts identified by the examiner are directed to these features of claim 8.

Malan also neither describes nor suggests determining if the number of ports used in the historical profile is considerably smaller by a factor "Cl" than a current number of ports being scanned by a host and the current number is greater than a lower-bound threshold "C2", to record the anomaly; and reporting a port scan whether at [0067-0068] or elsewhere. Again, Malan discusses comparing data statistics and does not suggest determining if the number of ports used in the historical profile is considerably smaller … than a current number of ports being scanned by a host … .

Claims 9-13 add distinct features and are also allowable over Malan.

Claims 14, 24, and 28 and dependent claims 15-19; 25-27; and 29-32 include analogous features as claim 1 and claims 2-7, and are thus allowable for analogous reasons.

Claims 20, 33 and dependent claims 21-23 and 34-36 include analogous features as claim 8 and claims 9-13, and are thus allowable for analogous reasons.

It is believed that all the rejections and/or objections raised by the examiner have been addressed.

In view of the foregoing, applicant respectfully submits that the application is in condition for allowance and such action is requested at the examiner's earliest convenience.

All of the dependent claims are patentable for at least the reasons for which the claims on which they depend are patentable.

Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

No fee is believed due. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 6/26/09

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906